УДК 811.111:004.77.056

Majeiko E., Vanik I.

How a Virtual Private Network Works

Belarusian National Technical University
Minsk, Belarus

Nowadays it is easy to track your activity on the Internet. Every time you connect to the Internet, your data and traffic passes through the ISP in a readable format. It turns out that the provider can see everything that you use on the Internet: what you are looking for, what files you download, what sites you visit, etc. For many people it is not really a problem, however, what if it will be a malefactor? Once they gain access to your connection (especially in unsecured networks), they can steal either money or personal data. Besides, your exact location can also be exposed through the IP.

In order to protect your data from the third parties a VPN was created. A VPN or Virtual Private Network is a technology that creates secure, encrypted connection of the user to the network, with which he can maintain privacy. To use a VPN, you just need to download an application. A VPN client is software from VPN service providers that allows users to use VPN services on their devices. These programs are usually very easy to install and set up and work on most devices and operating systems. In most cases, users just need to launch the client and select the server they want to connect to. In addition, you can configure some connection settings such as TCP/UDP connection type or select a VPN protocol.

When you turn on VPN the client starts to encrypt data to protect your connection and the traffic you receive from the internet. Simply put, encryption is a way of converting data from a readable format to an encoded one. Only the

person/device that has the decryption key (in this case, a VPN client and VPN server) can convert the data back into a readable format. It is worth noting that the level of encryption will depend on which protocol is used in the selected software. A lower level of encryption gives you more speed, but the protection is lower as well. At the same time, more powerful encryption protocols slow things down as the data is being encrypted all the time. After encryption, then client creates a "tunnel" of encrypted data between the appropriate server and ISP. Everyone outside the tunnel cannot look inside. Next, the VPN server replaces your IP address with its own (thus hiding your location) and starts decrypting the data it receives from you and forwards it to the Internet. It then encrypts the data it receives from the Internet and sends it to you. When the VPN client receives incoming traffic, it decrypts it for you.

VPN servers are ordinary servers with VPN software configured on them. They just have more logical and communication ports. VPN Services host their services on such servers and provide them to customers. VPN software provides access control system and secure connection between client and server using various types of VPN protocols. In addition, as soon as you connect to it, your ISP-provided IP address is replaced with the IP address of the VPN server. This way, any website you open while connected to the VPN server will only see the IP address of the VPN server [1].

But how to choose a VPN? First of all, you should look at privacy policies. Especially look whether they have no log policy. Quite often, companies indicate the fact of sale or distribution of your data in privacy page, many users don't bother reading it, though. Also, it is recommended to see who owns a VPN, because the same company may specialize in adware and hijacking. And more over, one company may be the owner of more than two VPN services.

Second, you should look for a VPN with a free trial as it allows a user to test it before buying. Of course, some may say that it is easier to use a free VPN, however, to keep and maintain servers, VPN providers need money and if they don't get this money from a user directly, then companies use other methods. If you use any form of free VPN service, it is highly unlikely that you're protected and there's a huge possibility that your data is being harvested and sold to the highest bidder.

It is also recommended to check connection protocols. For example, OpenVPN is a good choice and has an open code, meaning everyone may contribute in its development. IKEv2 and SSTP are also good choices, however they may be not compliable with your device. The worst choices are L2TP / IPSec and PPTP as they are old and insecure, more over it is proven that NSA has decryption keys for this protocol [2].

In conclusion, VPN services are used for many purposes. Companies often use it to create shared network. In this kind of network employees can work freely having access to all needed files and projects and all of this will be secure, so company's secrets won't leak. Ordinary people use it to maintain privacy, to protect their data, especially on Public Wi-Fi that doesn't have any protection at all. So, a VPN lets users hide their browser history and protect from cyber-criminals. But of course, one shall not forget to choose a VPN wisely [3]!

References:

1. How does a VPN work? [Electronic resource] – Mode of access: cactusvpn.com/beginners-guide-to-vpn/how-does-a-vpn-work/ – Date of access: 21.03.2022.
2. How to pick a good VPN [Electronic resource] – Mode of access: https://blog.windscribe.co - Date of access: 21.03.2022.
3. 9 Reasons Why Everyone Should Use A VPN [Electronic resource] – Mode of access: www.forbes.com – Date of access: 21.03.2022